

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

* * *

UNITED STATES OF AMERICA,

Case No. 2:17-cr-00306-JCM-PAL

Plaintiff,

v.

**REPORT OF FINDINGS AND
RECOMMENDATION**

JOHN TELUSMA,

(Mot Suppress – ECF No. 475)

Defendant.

Before the court is defendant John Telusma’s (“Telusma”) Motion to Suppress Evidence (ECF No. 475), which was referred to the undersigned pursuant to 28 U.S.C. § 636(b)(1)(B) and LR IB 1-4 of the Local Rules of Practice. The court has considered the motion, the government’s Opposition (ECF No. 515), and Telusma’s Reply (ECF No. 522).¹

BACKGROUND

I. THE INFRAUD INDICTMENT

Mr. Telusma (a.k.a. “John Westley Telusma,” “Peterelliot,” “Pete,” “Pette”) and 34 co-defendants are charged in a Second Superseding Indictment (ECF No. 303) (“Infraud indictment”) returned January 30, 2018.² This case arises out of allegations that the defendants operated a criminal organization known as the “Infraud Organization” (“Infraud”) in violation of the Racketeer Influenced and Corrupt Organizations Act (“RICO”), 18 U.S.C. §§ 1961–1968. Defendants allegedly engaged in identity theft and financial fraud with acts that include, but are

¹ Defendant Pius Wilson filed an omnibus Motion for Joinder (ECF No. 481) seeking to adopt the motions of his co-defendants to the extent any motion is applicable to him. The current motion argues that Choichiu’s Fourth Amendment rights were violated when the government executed a search warrant at his residence. Because Fourth Amendment rights are personal rights, they may not be vicariously asserted. *Rakas v. Illinois*, 439 U.S. 128, 133–34 (1978). Wilson does not specifically claim the search warrant or Chichiu’s arguments apply to him. Thus, Wilson’s joinder request is denied as to this motion. *See United States v. Lopez-Cruz*, 730 F.3d 803, 807 (9th Cir. 2013).

² A total of 36 defendants were named in the Infraud indictment. One defendant has been dismissed.

1 not limited to, money laundering, trafficking in stolen means of identification; trafficking in,
 2 production and use of counterfeit identification; identity theft; trafficking in, production and use
 3 of unauthorized and counterfeit access devices; bank fraud; and wire fraud, as well as services in
 4 connection with all of those acts. *Id.* at 6, ¶ 1.

5 Mr. Telusma is accused of being a “vendor,” providing “drop” services for other Infracred
 6 members as well as selling dumps. *Id.* at 16. “Vendors” (a.k.a. “Professors” or “Doctors”)
 7 allegedly sold illicit products and services to other Infracred members:

8 These sales may occur through the vendor’s own website, to which would-be
 9 purchasers are directed by the advertisements they pay for and place on the Infracred
 10 Organization’s web forum. Such sales may also occur directly between the vendor
 11 and customer, i.e. via email, [private message “PM”], or [instant messaging
 12 electronic communication service (“ICQ”) or “chat”]. Products sold by vendors
 are reviewed on the forum by Infracred members, to ensure that vendors of low-
 quality goods do not remain in business with the Organization. This helps to
 cement the Organization’s reputation as a premiere online destination for safe,
 high-quality and readily-available fraud-related contraband.

13 *Id.* at 13, ¶ 6.d.³

14 Telusma is charged in count one with racketeering conspiracy in violation of 18 U.S.C.
 15 § 1962(d). Count one alleges the defendants were employed by and associated with the Infracred
 16 “enterprise” and knowingly conspired to violate § 1962(c) by participating in a pattern of
 17 racketeering activity consisting of multiple acts indictable under 18 U.S.C. § 1028 (fraud and
 18 related activity in connection with identification documents, authentication features, and
 19 information), § 1029 (access device fraud), § 1343 (wire fraud), § 1344 (bank fraud), and § 1543
 20 (forgery or false use of passport). ECF No. 303 at 24, ¶ 12. With regard to overt racketeering acts,
 21 Telusma is accused as follows:

22 14.24 On or about August 18, 2011, **Telusma [16]** received in excess of 15
 23 compromised credit card numbers from **Unindicted Co-conspirator A**....

24 14.28 On or about September 15, 2011, **Unindicted Co-conspirator A** sent
Telusma [16] in excess of 15 compromised credit card dumps via email....

26 ³ Among other things, vendors allegedly sold “dumps,” which refers to compromised credit card account
 27 data, including an account holder’s name, date of birth, social security number, address, telephone number,
 28 and mother’s maiden name, as well as the security code on the back of the credit card. *Id.* at 8, ¶ 3.e–f. The
 term “drops” generally refers to protected drop sites, i.e., a location or individual able to securely receive
 and then forward retail items obtained via fraud. *Id.* ¶ 3.g.

14.109 On or about March 26, 2015, **Telusma [16]** requested via private message that **Bondarenko [1]** ban another Infraud member for “ripping” him on a deal.

Id. at 28, 37.

II. THE SEARCH WARRANTS

The motion to suppress addresses a single search warrant issued in the Eastern District of New York, executed February 6, 2018, authorizing the seizure of an iPad, a smartphone, a MacBook Pro, and non-electronic documents or records regarding ownership and/or possession of the searched premises located in Brooklyn, New York. The government’s response points out that at least *three* search warrants were issued in this investigation relating to Mr. Telusma. The suppression motion does not challenge the subsequent warrants. However, the court will briefly summarize the relevant portions of the affidavits submitted in support of the search warrant applications.

A. The First Warrant

On February 5, 2018, U.S. Magistrate Judge James Orenstein of the Eastern District of New York issued the first search and seizure warrant (“first warrant”) for the residence located at 42 Paerdegat 5th Street, Brooklyn, New York (“Brooklyn property”). *See* search and seizure warrant & application, Mot. Ex. A (ECF No. 475-1). Special Agent Lynda Interlandi (“SA Interlandi”) of Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”), submitted a 33-page affidavit in support of the application. SA Interlandi provided details of her training and experience on, among other things, cybercriminal organizations and electronic forensic evidence. *E.g., id.* at 19–21, 30–36.

The affidavit provides details of the Infraud indictment and the alleged racketeering conspiracy in furtherance of an online criminal carding organization known as Infraud.⁴ *Id.* at 14–20, 22–25. The affidavit indicates that Bondarenko was a member of the Carder.su criminal carding organization until he had a falling out with its leaders, broke ties and with co-defendant

⁴ As defined in the first warrant, “carding” means

the general concept of purchasing retail items with counterfeit credit cards or stolen credit card information. Such scheme may involve a counterfeit credit card that has been encoded with the legitimate victim account information, and is presented to a store’s cashier by the offender. Often, various false identification documents are used to facilitate this fraud....

ECF No. 475-1 at 8, ¶ I.3.a.

1 Medvedev formed the Infraud Organization, successfully recruiting Carder.su members to join
 2 him. Telusma provided “cashout”⁵ and drop services to other Infraud members, *id.* at 22, and the
 3 affidavit describes his alleged criminal activity in furtherance of the RICO conspiracy, *id.* at 24–
 4 25. His alleged racketeering acts include receiving in excess of 15 compromised credit card
 5 numbers in multiple emails from an unindicted co-conspirator in August and September 2011. In
 6 March 2015, he also requested via private message on the Infraud forum that the organization’s
 7 leader/indicted co-conspirator ban another Infraud member for “ripping” him on a deal.

8 SA Interlandi stated that the investigation revealed that Telusma had possession of several
 9 digital devices and continued to conduct carding activities. Based on this information, SA
 10 Interlandi believed that one or more of these devices would be located at the Brooklyn property.
 11 As relevant to this motion, she described:

12 35. On July 31, 2017, TELUSMA posted a photo with the caption “If your
 13 trying to make money... Here’s a gift from me, don’t forget where you got it!” The
 14 photo was of a chat screen displayed on a phone, involving an individual listed as
 15 “Monnaie INF,” with a message from that individual stating: “Hello! We made new
 shop to have better service. (CVV CCV CC Dumps) Updates every day. Choose
 stuff from lists we have in the shop.” That message included a link to the alleged
 online dumps shop.

16 36. On January 17, 2018, TELUSMA posted a photograph of himself that
 17 included a smartphone that he was holding, and a cell-phone holster he was
 wearing, in what appeared to be a residence.

18 37. In January 10, 2018, TELUSMA posted a photograph of a phone bill from
 Verizon, with the quote “What my phone bill be like.”

19 38. On August 26, 2017, TELUSMA posted a photograph of what appears to
 20 be an iPad in a residence.

21 *Id.* at 26–27. Based on SA Interlandi’s training and experience, and that of other federal agents,
 22 she stated:

23 individuals who commit electronic and Internet-based crimes, to include fraud and
 24 carding, generally possess multiple digital devices that they use to commit these
 crimes. Moreover, these individuals often retain old digital devices rather than sell
 25 them or dispose of them because they are aware that the devices contain contraband,
 and they do not wish to risk their criminal activity being discovered by the new

26
 27 ⁵ The term “cashout service” in the affidavit is used to “describe the transfer of funds, typically used in
 28 connection with obtaining and laundering illicitly obtained funds from compromised bank and credit card
 accounts. The members providing cashout services receive a fee, which is typically between five percent
 and ten percent of the total funds laundered.” ECF No. 475-1 at 10, ¶ I.3.n.

owner of their old devices, amongst other reasons. This is also the reason that such individuals own digital devices themselves, rather than using others' devices, as they do not wish to engage in their activities on digital devices owned by others and in doing so risk discovery.

Id. at 27–28, ¶ 40. Additionally,

Based on actual inspection of other evidence related to this investigation, including, among other things, email records, social media accounts, and other electronic communications, I am aware that computer equipment was used to access the Infraud Organization's forum, and to provide anonymous communications between members of the Organization in furtherance of the enterprise. Given that electronic communications played a significant factor in the furtherance of the enterprise, and that the individual residing at the [Brooklyn property] is a member of the Organization, there is reason to believe that there are computers and other digital devices currently located at the [Brooklyn property].

Id. at 31–32, ¶ 48.e.

SA Interlandi attested there was probable cause to believe a search of the Brooklyn property would lead to the discovery of evidence as fully described in Attachment B, "Property to be Seized." The attachment states the "items to be seized are the evidence, fruits, and instrumentalities" of 18 U.S.C. § 1962(d) (racketeering conspiracy), § 1028(a)(7) (identity theft), § 1029(a)(3) (possession of more than fifteen unauthorized access devices), § 1030 (computer fraud and related activity), § 1343 (wire fraud), § 1344 (bank fraud), and § 1956 (money laundering), specifically:

- a. An iPad, a smartphone, a MacBook Pro that may be used to access the Infraud Organization's forum via the Internet, and that may contain stored references to the Infraud nic "peterelliot," or to any other Infraud nic.⁶
- b. Any and all non-electronic documents or records regarding ownership and/or possession of the [Brooklyn property].

ECF No. 475-1 at 40.

Judge Orenstein issued the first warrant on February 5, 2018. *Id.* at 2. Federal agents executed this warrant at the Brooklyn property the following day. *Id.* at 5.

B. Supplemental Warrant

On February 6, 2018, Judge Orenstein issued a second search warrant ("supplemental warrant") for the Brooklyn property. *See* search and seizure warrant & application, Resp. Ex. A

⁶ The affidavit states that the term "nic" refers to "the screen name or nickname chosen by a member of the criminal organization by which that member will be known to other members." Mot. Ex. A (ECF No. 475-1) at 8, ¶ I.3.d.

(ECF No. 515-1). Special Agent Gregory P. Itsines (“SA Itsines”) of ICE/HSI submitted an affidavit in support of the supplemental warrant application, which incorporated the first warrant’s affidavit and provided additional facts supporting the request to seize additional evidence. Specifically, judicial authorization was sought to seize additional digital devices discovered during execution of the first warrant including an iPhone, an external hard drive, a MacBook Pro laptop, and a USB thumb drive as well as unused credit card “blanks,” which agents recognized were used in the creation of counterfeit credit cards, identification documents, and other access devices.

During the search of the Brooklyn property authorized by the first warrant, agents related how they identified Telusma’s bedroom where he was sleeping prior to their arrival. *Id.* at 3, ¶¶ 4–5. While searching his bedroom, SA Interlandi observed multiple digital devices, including an iPhone, external hard drive, and USB thumb drive. *Id.*, ¶ 6. SA Itsines represented, based on his training and experience:

I know that such items, specifically Iphones are used by individuals who are members of groups such as the Infraud Organization to access the organization’s “virtual clubhouse” on the Internet, to communicate with other members, to facilitate Internet-based criminal activity, and to store evidence related to such activity.

... [I]ndividuals who make counterfeit credit cards utilize external drives, such as thumb drives to store information related to manufacturing such.

Agent Interlandi also observed a box filled with unused, white credit card blanks, which I know from training and experience are used in the creation of counterfeit credit cards, identification documents, and other access devices.

Id., ¶¶ 7–9. Given these new facts, SA Itsines requested and received judicial authorization to seize evidence described in Attachment B, “Property to be Seized.” *Id.*, ¶ 10. The attachment stated the “items to be seized are the evidence, fruits, and instrumentalities” of 18 U.S.C. § 1962(d) (racketeering conspiracy), § 1028(a)(7) (identity theft), § 1029(a)(3) (possession of more than fifteen unauthorized access devices), § 1030 (computer fraud and related activity), § 1343 (wire fraud), § 1344 (bank fraud), and § 1956 (money laundering), specifically:

- a. A black Western Digital-brand “My Passport” external hard drive;
- b. A box of white unused credit card blanks;
- c. A black iPhone.

d. Any additional credit card making material: specifically credit card blanks, and holograms.

Attachment B, Notice of Corrected Doc. re: Resp. Ex. A (ECF No. 523) at 4.

Judge Orenstein approved the application for the supplemental warrant on February 6, 2018. *Id.* at 1. Federal agents executed the supplemental warrant later that day. *See* search warrant return & inventory sheet, Mot. Ex. A (ECF No. 475-1) at 3 & 5.

The first warrant and supplemental warrant authorized the search for and seizure of items, but did not authorize a search of the contents of the electronic devices. The digital devices were subsequently sent to the District of Nevada for use in this prosecution.

C. July 6 Warrants

On July 6, 2018, Magistrate Judge Carl W. Hoffman authorized the search of Telusma's digital devices seized at the Brooklyn property. *See* probable cause affidavit ("July 6 warrants"),⁷ Resp. Ex. B (ECF No. 515-1). Special Agent Michael Adams ("SA Adams") of ICE/HSI submitted the affidavit applying for the July 6 warrants. SA Adams described his training and experience on, among other things, use and manufacture of counterfeit credit cards, false identification documents, money laundering, unlicensed money remitting, racketeering, and wire fraud. *Id.* at 3–4.

SA Adams noted that Judge Orenstein issued the first warrant and supplemental warrant for Telusma's residence at the Brooklyn property. He incorporated both warrants by reference and attached them as Exhibits 1 and 2. He explained that agents executed the first warrant on February 6, 2018. During their execution of the first warrant, agents observed other items that, based on

///

///

///

⁷ The government's response refers to this third application as a single warrant. *See* Resp. (ECF No. 515) at 4. However, separate warrants were requested and received for each device, supported by an identical affidavit supporting probable cause to search the contents of each of the devices seized in pursuant to the two warrants issued in the Eastern District of New York. Thus, the court uses the plural: "July 6 warrants." Additionally, the court notes that the response did not attach the signed and approved version of the July 6 warrants. However, Telusma's reply does not dispute that the July 6 warrants were issued in the form attached to the government's response, or that the government disclosed images of his seized devices during Discovery Production 3 in October 2018. *See* Resp. at 4–5.

1 their training and experience, were credit card “blanks,” as well as numerous digital devices.⁸ The
 2 first warrant did not authorize the seizure of those devices. Agents therefore returned to Judge
 3 Orenstein that day and obtained a supplemental warrant authorizing seizure of the carding material
 4 and devices the agents observed in Telusma’s bedroom. Pursuant to the supplemental warrant,
 5 agents returned to the Brooklyn property on February 6 and seized his digital devices:

- 6 a. Western Digital 1TB External Hard Drive, serial number WXA1A359RCF0
- 7 b. Apple Macbook Laptop, serial number W89340K691T, containing HGST 500GB Hard Drive, Serial Number 3TJ2GS8H
- 8 c. Apple iPad Pro, serial number DLXVR057HPQJ
- 9 d. Apple iPhone 8 Plus, serial number F2MVD5G5JCLM
- 10 e. Apple iPhone X, serial number DNPVQ4Y1JCL7

11 *Id.* at 5. They also seized various credit card “blanks.” SA Adams knew, based on his training
 12 and experience:

- 13 a. Credit card “blanks” are blank credit card material utilized by carders to create fraudulent credit cards.
- 14 b. Digital devices, such as smart phones, computers, and various electronic storage media are necessary to obtain compromised credit and debit card information, and to facilitate the creation of fraudulent credit and debit cards and identifications using “blanks,” such as the ones found in the [Brooklyn property].

17 *Id.* at 5–6, ¶ 6.

18 SA Adams informed Judge Hoffman that the supplemental warrant did not authorize
 19 examination of the contents of Telusma’s devices, but only authorized their seizure. Agents from
 20 the Eastern District of New York did not examine the contents of the devices. SA Adams received
 21 the devices from those agents on March 13, 2018. At that time, SA Adams and his fellow agents
 22 assumed they “had a search warrant that not only authorized seizure of the DEVICES, but also
 23 examination of any seized devices.” *Id.* at 6, ¶ 8. Judge Hoffman was informed that between

24
 25 ⁸ The affidavit defines “digital devices” to include:

26 any electronic system or device capable of storing or processing data in digital form,
 27 including central processing units; forensic images of computers, desktop, laptop,
 28 notebook, and tablet computers; personal digital assistants; wireless communication
 devices, such as telephone paging devices, beepers, *mobile telephones*, and *smart phones*;
 digital cameras; [and] peripheral input/output devices....

Id. at 7–8, ¶ 12 (emphasis added).

1 April 2 and 18, 2018, Task Force Officer Taun Yurek imaged the devices and began his
 2 examination of their contents. *Id.*, ¶¶ 7–8. Due to other case priorities and digital device
 3 examinations, officer Yurek did not complete the examination. *Id.*, ¶ 8. There was no further
 4 examination of the devices from April 18 through the date of the application. *Id.*

5 On May 31, 2018, SA Adams discovered that the first warrant did not address examination
 6 of the devices, and that officer Yurek’s examination of the forensic images of the devices was
 7 likely not authorized by the first warrant as SA Adams had mistakenly believed. *Id.*, ¶ 9. Thus,
 8 SA Adams made the application for the July 6 warrants to authorize a search of Telusma’s devices
 9 seized pursuant to the supplemental warrant. SA Adams’s affidavit did not reveal any information
 10 learned by Yurek from the search of the seized devices.

11 Based on the facts set forth in the affidavit incorporating the facts described in the attached
 12 first warrant and supplemental warrant, SA Adams attested there was probable cause to believe
 13 that a search of Telusma’s devices would lead to the discovery of evidence as fully described in
 14 Attachment B, “Particular Things to be Seized.” *Id.* at 16–18. The attachment requested judicial
 15 authorization to seize: “[a]ll records relating to violations” of 18 U.S.C. § 1028(a)(1) (unlawful
 16 trafficking in and production of counterfeit identification documents or authentication features),
 17 § 1028(a)(7) (identity theft), § 1029(a)(3) (possession of more than fifteen unauthorized access
 18 devices), § 1030 (computer fraud and related activity), § 1343 (wire fraud), § 1344 (bank fraud),
 19 and § 1962(d) (racketeering conspiracy). *Id.* at 16. Specifically, records such as:

- 20 1. Records related to the Infraud Organization, to include records relating to
 21 the use and administration of the Organization’s forum, website, or other related
 servers, from the date of October 2010 to the present date.
- 22 2. Records constituting indicia of membership in the Infraud Organization,
 23 from the date of October 2010 to the present date.
- 24 3. Records related to the nic “PeterElliot” within the Infraud Organization and
 other carding organizations, from the date of October 2010 to the present date.
- 25 4. Records containing or otherwise pertaining to electronic communications
 26 regarding the Infraud Organization, other carding organizations, or the crimes of
 27 access device fraud, wire fraud, identity theft, bank fraud, money laundering,
 unauthorized computer access, and racketeering, from the date of October 2010 to
 the present date.
- 28 5. Records related to any other nic used within the Infraud Organization, or

1 used within other carding organizations on the Internet or dark web, from the date
2 of October 2010 to the present date....

3 ECF No. 515-2 at 16–17.

4 Judge Hoffman approved SA Adam’s application and issued the July 6 warrants on July 6,
5 2018. Resp. (ECF No. 515) at 4.

6 **III. THE PARTIES’ POSITIONS**

7 **A. The Motion to Suppress (ECF No. 475)**

8 Telusma’s motion asks the court to suppress evidence seized during a search at his
9 residence pursuant to the first warrant executed in the Eastern District of New York arguing the
10 warrant is overbroad and lacks particularity. He claims the first warrant is overbroad because it
11 authorizes the seizure of two iPhones, and the supporting affidavit did not articulate probable cause
12 to show that Telusma used a smartphone to facilitate the alleged fraudulent transactions. He claims
13 there is no evidence in the affidavit reflecting that Telusma used a smartphone or an iPhone to
14 participate on the Infraud forum. The affidavit contains two references to smartphones, which
15 may confirm that Telusma owned a cell phone but do not verify that he used a cell phone to
16 participate in the Infraud forum or that the cell phone he used was an iPhone. SA Interlandi
17 represented that, in her “training and experience . . . individuals who commit electronic and
18 Internet-based crimes, to include fraud and carding, generally possess multiple digital devices that
19 they use to commit these crimes.” Affidavit, Mot. Ex. A (ECF No. 475-1) at 27–28, ¶ 40. Telusma
20 claims this statement is “highly generalized and not particularly persuasive.” Mot. at 7. He
21 contends that for probable cause to exist, the affidavit must establish that Telusma: (1) must have
22 owned a cell phone; (2) that cell phone must have been an iPhone; and (3) that iPhone must have
23 been used to perpetrate the criminal activity under investigation. *Id.* at 6–7.

24 Alternatively, Mr. Telusma argues the first warrant failed to place practical limitations on
25 the agents’ discretion because it: (1) authorized seizure of evidence related to violations of seven
26 broad criminal statutes; (2) authorized seizure of devices instead of specific documents or files;
27 and (3) lacked any temporal limitation. With regard to “Property to be Seized,” Attachment B to
28 the affidavit states that the “items to be seized are the evidence, fruits and instrumentalities” of 18
U.S.C. § 1962(d) (racketeering conspiracy), § 1028(a)(7) (identity theft), § 1029(a)(3) (possession

1 of more than fifteen unauthorized access devices), § 1030 (computer fraud and related activity),
 2 § 1343 (wire fraud), § 1344 (bank fraud), and § 1956 (money laundering), “*specifically: a. An*
 3 *IPad, a smartphone, a MacBook Pro* that may be used to access the Infraud Organization’s forum
 4 via the Internet, and that may contain stored references to the Infraud nic ‘peterrelliot,’ or to any
 5 other Infraud nic”....⁹ Mot. Ex. A (ECF No. 475-1) at 4 (emphasis added).

6 Telusma asserts that “the reference to the criminal activity under investigation” represents
 7 the only limitation on the agents’ discretion in conducting the search. Mot. at 8. He contends the
 8 first warrant could have been more particular. For example, it could have requested seizure of
 9 “evidence relating to the purchase or sale of compromised credit cards,” “evidence of contacts
 10 with the Infraud forum,” or “evidence of contacts with Bondarenko or Medvedev (the alleged
 11 leaders of Infraud forum).” *Id.* at 9. Additionally, he argues the lack of time limitation would
 12 allow agents to review documents on these devices at any time, without regard to when the
 13 suspected criminal activity took place. This amounts to a wholesale rummaging through a person’s
 14 belongings, which the Fourth Amendment prohibits. The court should suppress evidence of the
 15 devices and all of the evidence gathered from the four seized devices.

16 **B. The government’s Response (ECF No. 515)**

17 In response, the government notes that Telusma’s arguments focus solely on the first
 18 warrant and ignore the supplemental warrant authorizing the seizure of the smartphones and other
 19 devices, and the July 6 warrants authorizing the search of those devices. Reading all these warrants
 20 together in context, the search and seizure of Telusma’s devices was lawful, and the fruits of the
 21 search should not be suppressed.

22 The government maintains that Judge Orenstein correctly found probable cause that
 23 Telusma’s smartphones contained evidence of criminal activity. The response points out that
 24 Telusma does not argue investigators lacked probable cause to believe he was involved in the
 25 crimes under investigation. Rather, he argues that probable cause did not exist to seize the two
 26

27 ⁹ The affidavit states that the term “nic” refers to “the screen name or nickname chosen by a member of
 28 the criminal organization by which that member will be known to other members.” Mot. Ex. A (ECF
 No. 475-1) at 8, ¶ I.3.d.

1 iPhones. However, the supplemental warrant authorized seizure of the iPhones after agents
2 discovered those phones in Telusma's bedroom during execution of the first warrant. Resp. at 6.

3 The government also asserts there was probable cause to believe Telusma's cell phones
4 were likely used to commit crimes, and likely contained evidence of those crimes. The affidavit
5 for the first warrant showed that Telusma was engaged in a number of electronic and Internet-
6 based crimes that require the use of digital devices to commit. "Because the Defendant must have
7 used digital devices to commit his crimes, it was reasonable to seek evidence of those crimes on
8 any digital devices that the Defendant owned, including the iPhones." *Id.* at 7. Smartphones, such
9 as an iPhone, can be used to access criminal carding forums like Infraud and to communicate with
10 co-conspirators. Additionally, digital devices often store historical information related to criminal
11 activity from before a device became operational, *e.g.*, imported contacts or email from another
12 phone. Telusma argues there was no probable cause to seize the iPhone X because it was
13 "released" by Apple, *i.e.*, available for sale, in early November 2017, but the Infraud indictment
14 was not returned until January 30, 2018, nearly three months later. However, Infraud's members
15 allegedly continued to commit crimes in furtherance of the racketeering conspiracy through the
16 date of the Infraud indictment. Thus, it was reasonable to conclude the iPhone X would contain
17 evidence of criminal activity.

18 Finally, the response asserts that the July 6 warrants provided practical limitations and
19 meaningful constraints on the search of Telusma's devices. Although the first warrant may not
20 have authorized seizure of any specific documents or files, the July 6 warrants authorizing a search
21 of the contents of the devices that yielded the incriminating evidence Telusma seeks to suppress
22 did. The July 6 warrants authorized the seizure of 10 specific categories of records relevant to the
23 specific criminal violations referenced in the affidavit from October 2010 to the present.

24 For these reasons, the court should deny Telusma's suppression motion.

25 **C. Mr. Telusma's Reply (ECF No. 522)**

26 The reply contends that Telusma's suppression motion turns on the level of connection
27 required between the items the government seeks to seize and the crime under investigation. He
28 claims the government improperly relies on an assumption that Telusma *must have* used digital

1 devices to commit his alleged crimes, rather than articulating a tangible and articulable nexus
 2 between the crimes alleged and the devices seized. Probable cause to search required a connection
 3 between the crime alleged and the digital devices to be seized. Reading the affidavits in the light
 4 most favorable to the government, Telusma argues the government “has no idea how Telusma
 5 allegedly accessed the Infraud forum – whether through a laptop, a tablet, a smartphone, or a
 6 desktop at the local library.” Reply at 3. The government was required tie the particular device
 7 to the crime alleged. Instead, Telusma claims the government sought “seizure of every device,
 8 found in any location, with any alleged connection to Telusma - no matter how tenuous - ... so
 9 long as there was some possibility - no matter how remote - Telusma could have used it to initiate
 10 contact with the internet.” *Id.* at 3–4.¹⁰

11 In addition, Telusma asserts that the transferrable nature of digital evidence requires the
 12 government to identify at least one device that Telusma used to access the Infraud forum and on
 13 which evidence is likely to be found. Although it is possible that a person may transfer data from
 14 one device to another, the mere possibility does not establish probable cause or provide the
 15 requisite link between the particular device to be seized and the alleged crime. Accordingly,
 16 Telusma asks the court to suppress the evidence resulting from the digital devices seized on
 17 February 6, 2018.

18 DISCUSSION

19 **I. APPLICABLE LEGAL STANDARDS**

20 The Fourth Amendment secures “the right of the people to be secure in their persons,
 21 houses, papers, and effects against unreasonable searches and seizures.” U.S. Const. amend. IV.
 22 Evidence obtained in violation of the Fourth Amendment, and evidence derived from it may be

23 ¹⁰ In a long footnote, Mr. Telusma argues the record is unclear about what device was found during two
 24 possible searches of the Brooklyn property. *Id.* at 4 n.4. He acknowledges that the first warrant plainly
 25 “authorized the government to seize *an iPhone* and the MacBook Pro, if such devices were located.” *Id.*
 26 (emphasis added). The affidavit supporting the supplemental warrant states that SA Interlandi “observed
 27 *an iPhone*” on Telusma’s bed, *id.* (citing Feb. 6 warrant ¶ 6), but does not specify whether it was an iPhone
 28 8 or iPhone X, and the agents prepared a single inventory of items seized for both searches. Mr. Telusma
 claims the government should be ordered to clarify which iPhone was found during which search and where
 in the house. Furthermore, even if agents located an iPhone in Telusma’s bedroom, that fact “does not
 establish that this particular device - whichever iPhone it was - was used to access the online forum and it
 provides absolutely no nexus between *the other iPhone* and the crime alleged.” *Id.*

1 suppressed as the “fruit of the poisonous tree.” *Wong Sun v. United States*, 371 U.S. 471, 484–87
 2 (1963); *United States v. Lundin*, 817 F.3d 1151, 1157 (9th Cir. 2016); *United States v. McClendon*,
 3 713 F.3d 1211, 1215 (9th Cir. 2013) (“Searches and seizures that offend the Fourth Amendment
 4 are unlawful and evidence obtained as a direct or indirect result of such invasions is considered
 5 ‘fruit of the poisonous tree’ and is inadmissible under the exclusionary rule.”).

6 The Fourth Amendment’s Warrant Clause provides that a warrant may be issued only
 7 “upon probable cause, supported by Oath or affirmation, and particularly describing the place to
 8 be searched, and the persons or things to be seized.” U.S. Const. amend. IV. This language
 9 imposes three requirements. *Dalia v. United States*, 441 U.S. 238, 255 (1979). A valid search
 10 warrant must be: (1) issued by a neutral and detached judge; (2) supported by probable cause to
 11 believe the evidence sought will aid in a particular apprehension or conviction for a particular
 12 offense; and (3) describe the things to be seized and the place to be searched with particularity.
 13 *United States v. Artis*, --- F.3d ---, 2019 WL 1375260, at *3 (9th Cir. Mar. 27, 2019) (citing *Dalia*,
 14 441 U.S. at 255).

15 **A. Probable Cause**

16 The probable cause standard is a fluid and nontechnical concept that is incapable of precise
 17 definition or quantification. *Maryland v. Pringle*, 540 U.S. 366, 370–71 (2003); *United States v.*
 18 *Hill*, 459 F.3d 966, 972 (9th Cir. 2006) (probable cause is “not readily susceptible to multifactor
 19 tests or rebuttable presumptions”). “Probable cause exists where the totality of the circumstances
 20 indicates a ‘fair probability that . . . evidence of a crime will be found in a particular place’.”
 21 *United States v. Elmore*, 917 F.3d 1068, 1074 (9th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S.
 22 213, 238 (1983)); *United States v. Alaimalo*, 313 F.3d 1188, 1193 (9th Cir. 2002) (probable cause
 23 requires only a fair probability or substantial chance of criminal activity). “This standard does not
 24 require the affidavit to establish that the evidence is in fact in the place to be searched, or even that
 25 it is more likely than not to be there.” *Elmore*, 917 F.3d at 1074 (citing *United States v. Fernandez*,
 26 388 F.3d 1199, 1254 (9th Cir. 2004)); *United States v. Kelley*, 482 F.3d 1047, 1050 (9th Cir. 2007)
 27 (neither certainty nor a preponderance of the evidence is required). “Rather, the issuing judge
 28 ‘need only conclude that it would be reasonable to seek the evidence in the place indicated in the

1 affidavit’.” *Elmore*, 917 F.3d at 1074 (quoting *Fernandez*, 388 F.3d at 1254).

2 It is well recognized that law enforcement officers can rely on their own experience, and
 3 the experience and information of other law enforcement officers, in establishing probable cause.
 4 *United States v. Butler*, 74 F.3d 916, 920–21 (9th Cir. 1996). An officer’s “first hand knowledge”
 5 of a defendant’s criminal conduct, combined with the officer’s “experience” with other individuals
 6 who committed similar crimes, provides a “substantial basis” for a magistrate judge to determine
 7 that probable cause exists. *United States v. Johnson*, 913 F.3d 793, 802 (9th Cir. 2019) (citing
 8 *United States v. Terry*, 911 F.2d 272, 275–76 (9th Cir. 1990)). Similarly, a magistrate judge “ ‘may
 9 rely on the conclusions of experienced law enforcement officers regarding where evidence of a
 10 crime is likely to be found’.” *Fernandez*, 388 F.3d at 1253 (quoting *Terry*, 911 F.2d at 275).

11 **B. Specificity**

12 Search warrants must be specific. *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006).
 13 “Specificity has two aspects: particularity and breadth. Particularity is the requirement that the
 14 warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the
 15 warrant be limited by the probable cause on which the warrant is based.” *Id.* (citing *United States*
 16 *v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993)).

17 1. Particularity

18 The purpose of the particularity requirement is to prevent general searches. *Maryland v.*
 19 *Garrison*, 480 U.S. 79, 84 (1987). By limiting the authorization to search the specific areas and
 20 things for which there is probable cause to search, the particularity requirement ensures that the
 21 search will be carefully tailored to its justifications, and will not become a wide-ranging,
 22 exploratory search that the Fourth Amendment prohibits. *Id.*; *In re Search of Google Email*
 23 *Accounts identified in Attachment A*, 92 F. Supp. 3d 944, 950 (D. Alaska 2015) (citing *Payton v.*
 24 *New York*, 445 U.S. 573, 584 n.21 (1980) (retracing the roots of the particularity requirement to
 25 the colonialists’ objections to the writs of assistance)). The particularity requirement also prevents
 26 “exploratory rummaging in a person’s belongings.” *United States v. Rodriguez*, 869 F.2d 479, 486
 27 (9th Cir. 1989) (citing *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)). The need to prevent
 28 general exploratory rummaging of a person’s belongings is particularly acute in document searches

1 because, unlike requests for other tangibles, document searches tend to involve broad disclosures
 2 of the intimacies of private lives, thoughts, and transactions. *United States v. Washington*, 797
 3 F.2d 1461, 1468 (9th Cir. 1986). However, the Ninth Circuit has often recognized a legitimate
 4 law enforcement need to scoop up large quantities of data and sift through it carefully for concealed
 5 or disguised pieces of evidence. *See, e.g., Hill*, 459 F.3d at 973.

6 To satisfy the particularity requirement the “description must be specific enough to enable
 7 the person conducting the search reasonably to identify the things authorized to be seized.” *United*
 8 *States v. Fries*, 781 F.3d 1137, 1151 (9th Cir. 2015) (quoting *United States v. Smith*, 424 F.3d 992,
 9 1004 (9th Cir. 2005)). In determining whether a warrant is sufficiently particular, the Ninth Circuit
 10 considers one or more of the following factors: (1) whether probable cause exists to seize all items
 11 of a particular type described in the warrant; (2) whether the warrant sets out objective standards
 12 by which the executing officers can differentiate items subject to seizure from those which are not;
 13 and (3) whether the government was able to describe the items more particularly in light of the
 14 information available to it at the time the warrant was issued. *See, e.g., United States v. Turner*,
 15 770 F.2d 1508, 1510 (9th Cir. 1985).

16 The warrant’s description of items need only be “reasonably specific, rather than
 17 elaborately detailed.” *Hill*, 459 F.3d at 973 (citing *United States v. Storage Spaces Designated*
 18 *Nos. 8 & 49*, 777 F.2d 1363, 1368 (9th Cir. 1985)). “Warrants which describe generic categories
 19 of items are not necessarily invalid if a more precise description of the items subject to seizure is
 20 not possible.” *Id.* The level of specificity required “varies depending on the circumstances of the
 21 case and the type of items involved.” *Id.*; *see also United States v. Spilotro*, 800 F.2d 959, 963
 22 (9th Cir. 1986) (detail necessary in a warrant is related to particular circumstances and nature of
 23 evidence sought). “[T]he scope of a lawful search is ‘defined by the object of the search’.” *United*
 24 *States v. Ewain*, 88 F.3d 689, 692 (9th Cir. 1996) (quoting *Garrison*, 480 U.S. at 84). The test is
 25 an objective one: “would a reasonable officer have interpreted the warrant to permit the search at
 26 issue.” *United States v. Gorman*, 104 F.3d 272, 274 (9th Cir. 1996); *see also United States v.*
 27 *Leon*, 468 U.S. 897, 918–19 (1984); *United States v. Traylor*, 656 F.2d 1326, 1331 (9th Cir. 1981).

28 ///

2. Breadth Requirement

“The purpose of the breadth requirement is to limit the scope of the warrant by the probable cause on which the warrant is based.” *Fries*, 781 F.3d at 1151 (quoting *Smith*, 424 F.3d at 1004); *see also Hill*, 459 F.3d at 973 (“ ‘Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based’.”) (quoting *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993)). Stated differently, “overbreadth is a tailoring question: does the proposed warrant limit the government’s search to the specific places that must be inspected to confirm or dispel the suspicion that gave rise to probable cause?” *In re Search of Google Email*, 92 F. Supp. 3d at 950 (citing *Garrison*, 480 U.S. at 84 (“By limiting the authorization to search to the *specific areas* and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wire-ranging exploratory searches the Framers intended to prohibit.”) (emphasis added)); *see also United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982); Wayne R. LaFare, *Search and Seizure: A Treatise on the Fourth Amendment* § 3.7(d) at 546 (5th ed. 2012) (describing overbreadth as the “object-place nexus” issue, and noting that the problem arises when a search warrant describes “the place be searched in broader terms than is justified by the probable cause showing in the affidavit.”).

C. Standard of Review for Search Warrants

The Supreme Court established the standard of review for the issuance of a search warrant in *Illinois v. Gates*, 462 U.S. 213 (1983). The issuing magistrate judge must make a practical, common-sense decision whether, given totality of the circumstances set forth in the affidavit, including the veracity and basis of knowledge of people supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place. *Id.* at 238. A reviewing court has a duty to ensure that the magistrate judge had a “substantial basis” for concluding that probable cause existed. *Ewing v. City of Stockton*, 588 F.3d 1218, 1223 (9th Cir. 2009) (citing *Gates*, 462 U.S. at 238–39). In doubtful cases, the court should give preference to the validity of the warrant. *Kelley*, 482 F.3d at 1050–51 (citing *Gates*, 462 U.S. at 237 n.10). The court should not “flyspeck” the affidavit supporting a search warrant through de novo review;

1 instead, the magistrate's determination "should be paid great deference." *Id.* at 1051 (citing *United*
2 *States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006) (en banc)). As a result, a judge's
3 determination that an affidavit provided probable cause to issue a search warrant "will be upheld
4 unless clearly erroneous." *United States v. Alvarez*, 358 F.3d 1194, 1203 (9th Cir. 2004).

5 **II. ANALYSIS AND DECISION**

6 Reviewing the affidavit as a whole, applying the totality of the circumstances test, and
7 showing the issuing judge great deference as the Supreme Court requires, the court concludes the
8 issuing magistrate judge had a substantial basis for concluding that probable cause existed to issue
9 the first warrant. The affidavit informed Judge Orenstein about SA Interlandi's training and
10 experience in cybercriminal organizations and electronic forensic evidence. Judge Orenstein was
11 allowed to rely on SA Interlandi's extensive training and experience in making his decisions.

12 The first warrant's affidavit describes the internet-based Infraud organization, the charges
13 against Mr. Telusma, and his alleged conduct. SA Interlandi carefully described her reasons to
14 believe Telusma was residing at the Brooklyn property and why evidence would be found there.
15 The affidavit also provides detailed explanations of why SA Interlandi believed, based on
16 information learned during the investigation and her training and experience, that Telusma would
17 have an iPad, a smartphone, and MacBook Pro on which evidence of the racketeering conspiracy
18 and overt acts would likely be found. SA Interlandi's representations sufficiently articulated her
19 reasons for believing that Telusma used internet-enabled digital devices, including a smartphone,
20 to facilitate the alleged fraudulent transactions. Telusma does not contend that his devices lacked
21 the capability of connecting to the internet and/or sending electronic communications. The court
22 finds that SA Interlandi's affidavit provided sufficient probable cause to search for Telusma's
23 devices.

24 Mr. Telusma claims the first warrant could have been more particular because it did not
25 specify that his smartphone was an iPhone or specify the iPhone model. However, there is no
26 indication that agents involved in the Infraud investigation were aware of what type of smartphone
27 Telusma used at the time the first warrant was issued. The affidavit related that the crimes under
28 investigation were committed over the internet using digital devices and that Telusma was

1 photographed using a smartphone and wearing a cell phone holster and he posted information
2 about his cell phone bill to Facebook. *See Spilotro*, 800 F.2d at 963 (considering whether
3 government was able to describe items more particularly in light of information available to it at
4 the time the warrant was issued). The first warrant requested judicial authorization to seize an
5 iPad, a smartphone and a MacBook Pro. SA Interlandi's affidavit meticulously explained how
6 investigators were able to identify Telusma and the email account and "nics" he was using to
7 participate in Infracore's crimes. She attested how she knew Telusma was in control of an Infracore
8 "nic" and registration email account. She attested that investigators discovered several instances
9 of Telusma receiving compromised credit card numbers on this email account, and that multiple
10 emails sent from the account indicated the emails were "sent from my iPad."

11 The affidavit for the first warrant also related that Telusma posted a photograph of himself
12 using a smartphone, and a cell phone holster he was wearing, a Verizon phone bill, and what
13 appeared to be an iPad in a residence. Telusma also posted a photograph of a MacBook Pro with
14 the quote "I love this 'Mac', I spent 5k on it when it first came out. It help me make thousands till
15 this day. I'll never get rid of it. It has made its way into my 'Hall of Fame' ..." ECF No. 475 at
16 27, ¶ 39. The request to seize an iPad, a smartphone and a MacBook Pro was clearly based on
17 information learned in the investigation, and stated as specific a description as investigators could
18 provide. *See Fries*, 781 F.3d at 1151 (requiring a specific enough description "to enable the person
19 conducting the search reasonably to identify the things authorized to be seized"). The first warrant
20 was reasonably tailored to seize devices Telusma was allegedly using to commit the cybercrimes
21 described. The devices were described with as much particularity as possible based on what
22 investigators knew at the time. Moreover, the fact that the supplemental warrant was requested
23 and received demonstrates that the first warrant was not overbroad. When officers executing the
24 search for three devices found credit card blanks used to create counterfeit credit cards and other
25 identification documents and additional digital devices, they sought and obtained another warrant.
26 The supplemental warrant specifically described the additional devices found in Telusma's
27 bedroom with the credit card blanks and why investigators believed these devices would have
28 evidence of the enumerated offenses on them.

1 Telusma’s motion to suppress challenges only the first warrant issued for three electronic
2 devices. The first warrant also authorized seizure of non-electronic documents or records showing
3 control of the searched premises.¹¹ Rather, Telusma argues that the first warrant was overbroad
4 and lacked specificity because it did not limit the scope of the search of the contents of the devices.
5 However, the electronic devices seized pursuant to the first warrant and supplemental warrant were
6 not searched until they were returned to this district for use in this prosecution. Telusma does not
7 claim the warrants issued by Judge Hoffman in July 2018 were overbroad or lacking in
8 particularity. The July 6 warrants limited the search to evidence of the crimes at issue in this
9 prosecution on the devices seized pursuant to the first warrant and supplemental warrant from
10 October 2010 through the date the warrants were issued. Telusma does not claim that the
11 government intends to use electronic data found on the electronic devices searched pursuant to the
12 July 6 warrants outside the scope of what Judge Hoffman authorized.

13 The Ninth Circuit has repeatedly acknowledged that over-seizing “is an accepted reality in
14 electronic searching because there is no way to be sure exactly what an electronic file contains
15 without somehow examining its contents.” *United States v. Flores*, 802 F.3d 1028, 1044–45 (9th
16 Cir. 2015) (quoting *United States v. Comprehensive Drug Testing, Inc.* (“CDT”), 621 F.3d 1162,
17 1177 (9th Cir. 2010) (en banc)) (internal quotation and alteration omitted). Data that individuals
18 used to keep in file cabinets in physical facilities are now routinely stored electronically, and law
19 enforcement faces many challenges in retrieving electronically stored information. *CDT*, 621 F.3d
20 at 1175. Additionally, digital files are easy to disguise or rename; thus, were courts to limit a
21 warrant to a narrow search protocol, “much evidence could escape discovery” simply because a
22 defendant can mislabel the files documenting his criminal activity. *United States v. Adjani*, 452
23 F.3d 1140, 1150 (9th Cir. 2006). Because of the challenges involved in searches of electronically
24 stored information, the Ninth Circuit has recognized law enforcement’s “legitimate need to scoop
25 up large quantities of data, and sift through it carefully for concealed or disguised pieces of
26

27 ¹¹ The motion to suppress does not claim that the agents’ seizure of non-electronic records was overbroad
28 undoubtedly because the search warrant return indicates the executing agents seized only three pieces of
mail addressed to Telusma at the searched premises.


1 evidence.” *CDT*, 621 F.3d at 1176.¹²

2 Based on factual and practical considerations of everyday life on which reasonable and
 3 prudent people act, the evidence presented in the affidavit supporting the first warrant established
 4 the probability that evidence of Telusma’s crimes would be found at the Brooklyn property, the
 5 premises to be searched, on Telusma’s digital devices, the property to be seized and to be searched.
 6 *See Gates*, 462 U.S. at 235 (“only the probability, and not a prima facie showing of criminal
 7 activity, is the standard of probable cause”). The first warrant was neither overbroad nor lacking
 8 in specificity. The court therefore finds that the issuing magistrate judge had a substantial basis
 9 for concluding that probable cause existed. Telusma’s Fourth Amendment rights were not violated.

10 For these reasons,

11 **IT IS RECOMMENDED** that defendant John Telusma’s Motion to Suppress Evidence
 12 (ECF No. 475) be **DENIED**.

13 DATED this 15th day of April 2019.

14
 15 
 16 PEGGY A. LEEN
 17 UNITED STATES MAGISTRATE JUDGE
 18
 19
 20
 21
 22
 23
 24

25 ¹² The Ninth Circuit has also repeatedly rejected overbreadth arguments that a search warrant should have
 26 authorized a pinpointed search and seizure of digital devices and data rather than a wholesale search. *E.g.*,
 27 *Flores*, 802 F.3d at 1044 (rejecting overbreadth argument where “only approximately 100 pages were truly
 28 responsive to the warrant” that authorized to search and seizure of “all 11,000 pages of data” in a Facebook
 account); *Adjani*, 452 F.3d at 1149–50 (requiring “a pinpointed computer search, restricting the search to
 an email program or to specific search terms, would likely have failed to cast a sufficiently wide net to
 capture the evidence sought.”).